

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

| | | | | |
|---|------------------------|---------------------------|------------|--|
| INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99) | Application Number | | 10628729 | |
| | Filing Date | | 2003-07-28 | |
| | First Named Inventor | Anne Kirsten Eisentraeger | | |
| | Art Unit | 2136 | | |
| | Examiner Name | CARL G COLIN | | |
| | Attorney Docket Number | MS1-1280US | | |

U.S. PATENTS

| Examiner Initial* | Cite No | Patent Number | Kind Code ¹ | Issue Date | Name of Patentee or Applicant of cited Document | Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear |
|-------------------|---------|---------------|------------------------|------------|---|--|
| | 1 | 6446205 | | 2002-09-03 | Lenstra | |

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S. PATENT APPLICATION PUBLICATIONS

| Examiner Initial* | Cite No | Publication Number | Kind Code ¹ | Publication Date | Name of Patentee or Applicant of cited Document | Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear |
|-------------------|---------|--------------------|------------------------|------------------|---|--|
| | 1 | | | | | |

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

| Examiner Initial* | Cite No | Foreign Document Number ³ | Country Code ² j | Kind Code ⁴ | Publication Date | Name of Patentee or Applicant of cited Document | Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear | T ⁵ |
|-------------------|---------|--------------------------------------|-----------------------------|------------------------|------------------|---|--|--------------------------|
| | 1 | | | | | | | <input type="checkbox"/> |

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

| Examiner Initials* | Cite No | Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published. | T ⁵ |
|--------------------|---------|---|----------------|
| | | | |

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

| | |
|------------------------|---------------------------|
| Application Number | 10628729 |
| Filing Date | 2003-07-28 |
| First Named Inventor | Anne Kirsten Eisentraeger |
| Art Unit | 2136 |
| Examiner Name | CARL G COLIN |
| Attorney Docket Number | MS1-1280US |

| | | |
|----|---|--------------------------|
| 1 | BARRETO, PAULO S.L.M., et al., "Efficient Algorithms for Pairing-Based Cryptosystems," Universidade de Sao Paulo, Escola Politecnica, Sao Paulo (SP), Brazil & Computer Science Department, Stanford University, USA, pp. 1-16. | <input type="checkbox"/> |
| 2 | Boneh, et al., "Identity-Based Encryption from the Weil Pairing," SIAM J. COMPUT., Vol 32, No. 3, pp. 586-615, 2003 Society for Industrial and Applied Mathematics. | <input type="checkbox"/> |
| 3 | Boneh et al., "Short signatures from the Weil pairing," pp. 1-17. | <input type="checkbox"/> |
| 4 | Cantor, "Computing in the Jacobian of a Hyperelliptic Curve," Mathematics of Computation, Vol. 48, No. 177, January 1987, pp. 95-101. | <input type="checkbox"/> |
| 5 | Eisentrager, et al., "Fast Elliptic Curve Arithmetic and Improved Weil Pairing Evaluation," Topics in Cryptology, CT-RSA 2003, Marc Joye (Ed), pp. 343-354, LNCS 2612, Springer-Verlag, 2003. | <input type="checkbox"/> |
| 6 | FREY, GERHARD et al., "A Remark Concerning m-Divisibility and the Discrete Logarithm in the Divisor Class Group of Curves," Mathematics of Computation, Vol. 62, No. 206, April 1994, pp. 865-874. | <input type="checkbox"/> |
| 7 | Galbraith, et al., "Implementing the Tate Pairing," Mathematics Dept., Royal Holloway, University of London, Egham, Surrey, UK & Hewlett-Packard Laboratories, Bristol, Filton Road, Stoke Gifford, Bristol, UK, pp. 1-14. | <input type="checkbox"/> |
| 8 | HESS, FLORIAN et al., "Two Topics in Hyperelliptic Cryptography," S. Vaudenay & A. Youssef (Eds.): SAC 2001, LNCS 2259, 2001, pp. 181-189. | <input type="checkbox"/> |
| 9 | JOUX, "The Weil and Tate Pairings as Building Blocks for Public Key Cryptosystems (Survey)," C. Fieker and D.R. Kohel (eds.): ANTS 2002, LNCS 2369, pp. 20-32, 2002 (Springer-Verlag Berlin Heidelberg 2002). | <input type="checkbox"/> |
| 10 | MENEZES, ALFRED J., et al., "Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field," (0018-9448/93 1993 IEEE, IEEE Transactions on Information...), 8 pages. | <input type="checkbox"/> |

If you wish to add additional non-patent literature document citation information please click the Add button

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

| | |
|------------------------|---------------------------|
| Application Number | 10628729 |
| Filing Date | 2003-07-28 |
| First Named Inventor | Anne Kirsten Eisentraeger |
| Art Unit | 2136 |
| Examiner Name | CARL G COLIN |
| Attorney Docket Number | MS1-1280US |

EXAMINER SIGNATURE

| | | | |
|--------------------|--|-----------------|--|
| Examiner Signature | | Date Considered | |
|--------------------|--|-----------------|--|

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

| | |
|------------------------|---------------------------|
| Application Number | 10628729 |
| Filing Date | 2003-07-28 |
| First Named Inventor | Anne Kirsten Eisentraeger |
| Art Unit | 2136 |
| Examiner Name | CARL G COLIN |
| Attorney Docket Number | MS1-1280US |

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

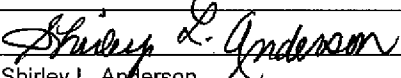
☐ See attached certification statement.

☒ Fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☐ None

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

| | | | |
|------------|---|---------------------|------------|
| Signature |  | Date (YYYY-MM-DD) | 2007-05-18 |
| Name/Print | Shirley L. Anderson | Registration Number | 57763 |

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**